PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-250570
(43)Date of publication of application : 17.09.1999

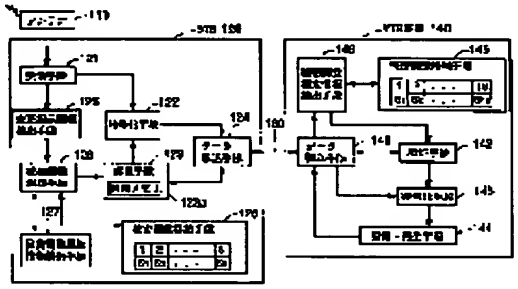
(51)Int.Cl. G11B 20/10
H04N 7/16

(21)Application number : 10-048221
(22)Date of filing : 27.02.1998

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : YAMADA MASAZUMI
IIZUKA HIROYUKI
TAKECHI HIDEAKI
GOTO SHOICHI

(54) SECRET INFORMATION CHANGING SYSTEM, SECRET INFORMATION CHANGING FIRST DEVICE, SECRET INFORMATION CHANGING SECOND DEVICE, AND MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a secret information changing system, a secret information changing 1st device, a secret information changing 2nd device, and a medium in which demerit caused by eliminating an illegal device can be made less than a conventional device.
SOLUTION: A STB converting a received broadcasting radio wave to AV data and the like is provided with a receiving means 121, a change indication information detecting means 125 detecting only change indication information from a received signal, a secret function selecting means 128 adding contents of a secret function history information storing means 127 by indication of the change indication information detecting means 125, selecting a new secret function from a secret function storing means 126, and changing a secret function being used now to the other secret function, an authentication means 123 using the selected secret function, and the like, and a VTR device 140 connected with a transmitting line 160 is provided with a secret function indication information extracting means 146 detecting discrimination number information out of transmitted signals, extracting a corresponding secret function from a secret function storing means 145 and outputting it to an authentication means 142, a decoding means 143, and the like.



LEGAL STATUS

[Date of request for examination] 26.02.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－250570

(43)公開日　平成11年(1999)９月17日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ
Ｈ０４Ｎ　7/16		Ｈ０４Ｎ　7/16	Ａ

審査請求　未請求　請求項の数18　ＯＬ　（全 12 頁）

(21)出願番号　特願平10－48221

(22)出願日　平成10年(1998)２月27日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　山田　正純
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　飯塚　裕之
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　武智　秀明
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　弁理士　松田　正道

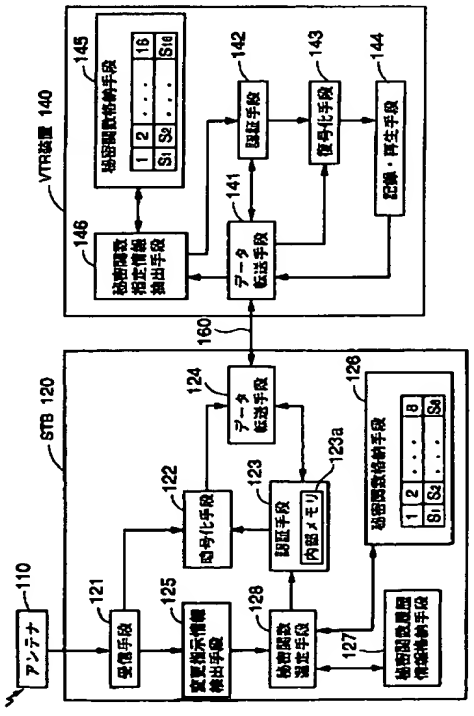
最終頁に続く

(54)【発明の名称】　秘密情報変更システム、秘密情報変更第１装置、秘密情報変更第２装置、及び媒体

(57)【要約】

【課題】不正装置の使用を阻止するために、悪用されたその秘密関数Ｓを使用しないようにすると、正規の装置までも使用出来なくなるという弊害が有った。

【解決手段】受信した放送電波をＡＶデータ等に変換するＳＴＢは、受信手段１２１と、受信信号から変更指示情報のみを検出する変更指示情報検出手段１２５と、変更指示情報検出手段１２５の指示で秘密関数履歴情報格納手段１２７の内容を加味して、秘密関数格納手段１２６から新たな秘密関数を選定し、現在使用中の秘密関数を別の秘密関数に変更する秘密関数選定手段１２８と、その選定された秘密関数を用いる認証手段１２３等を備え、伝送ライン１６０により接続されたＶＴＲ装置１４０は、伝送されてきた信号の中から識別番号情報を検出し、秘密関数格納手段１４５から対応する秘密関数を抽出し、認証手段１４２へ出力する秘密関数指定情報抽出手段１４６と、復号化手段１４３等を備える。



【特許請求の範囲】

【請求項１】　認証又は所定の処理に利用する第１秘密情報を、予め複数個有する第１装置と、
前記複数個の第１秘密情報に対応する複数個の第２秘密情報の内、全部又は一部の第２秘密情報を有し、その第２秘密情報を利用して、前記第１装置との間で前記認証を、又は前記所定の処理に対応する処理を行う第２装置とを備え、
前記第１又は第２装置が利用していた前記第１又は第２秘密情報をどれに変更すべきであるかを伝える外部からの指示に基づいて、前記第１又は第２秘密情報が変更されるものであり、
前記外部からの前記指示を受けた一方の前記装置が、他方の前記装置に対して、前記指示に基づく前記秘密情報の変更を指示するものであることを特徴とする秘密情報変更システム。

【請求項２】　認証又は所定の処理に利用する第１秘密情報を、予め複数個有する第１装置と、
前記複数個の第１秘密情報に対応する複数個の第２秘密情報の内、全部又は一部の第２秘密情報を有し、その第２秘密情報を利用して、前記第１装置との間で前記認証を、又は前記所定の処理に対応する処理を行う第２装置とを備え、
前記第１又は第２秘密情報を変更すべき旨を伝える外部からの指示があった場合、前記第１又は第２装置が、前記秘密情報をどれに変更するかを選定するものであり、
前記外部からの前記指示を受けた一方の前記装置が、他方の前記装置に対して、前記指示に基づく前記秘密情報の変更を指示するものであることを特徴とする秘密情報変更システム。

【請求項３】　前記第２装置は、前記複数個の第２秘密情報の内、一部の第２秘密情報を有するものであり、
前記第２装置により使用されていた第２秘密情報を変更すべき旨を伝える外部からの指示に基づいて、前記第２装置が、自らが有する前記第２秘密情報の中の、どの第２秘密情報に変更するかを選定するものであり、
その第２装置が、前記選定結果に基づき、前記第１装置に対して前記第１秘密情報の変更を指示するものであることを特徴とする請求項２記載の秘密情報変更システム。

【請求項４】　前記第２装置が有する第２秘密情報の数が、前記第１装置が有する第１秘密情報の数と同じであり、
前記第１又は第２装置により使用されていた第１又は第２秘密情報を変更すべき旨を伝える外部からの指示があった場合は、前記第１又は第２装置が、自らが有する前記秘密情報の中の、どの秘密情報に変更するかを選定するものであり、且つ、その第１又は第２装置が、前記選定結果に基づき、前記第２又は第１装置に対して、前記第２又は第１秘密情報の変更を指示するものであることを特徴とする請求項２記載の秘密情報変更システム。

【請求項５】　前記第１又は第２装置で利用される前記第１又は第２秘密情報を管理する管理装置を備え、
前記外部からの指示は、前記管理装置から出される指示であり、且つ、その指示は、電波、又は電話回線を介して前記第１又は第２装置に送られることを特徴とする請求項１、３又は４記載の秘密情報変更システム。

【請求項６】　前記第１又は第２装置は、記録媒体を再生する再生手段を備え、
前記外部からの指示は、前記再生手段により再生される前記記録媒体中に記録された情報であることを特徴とする請求項１、３又は４記載の秘密情報変更システム。

【請求項７】　前記外部からの指示は、前記第１又は第２装置が有する第１又は第２秘密情報の内、秘密性が保持されなくなったものを除外した残りの秘密情報の中のどの秘密情報を利用すべきであるかという指示であることを特徴とする請求項１記載の秘密情報変更システム。

【請求項８】　前記第２装置は、前記複数個の第２秘密情報の内、一部の第２秘密情報を有するものであり、
前記管理装置は、前記複数の第１秘密情報の内、秘密性が保持されなくなったものを除外した残りの第１秘密情報の中から、どれかを採用して、それらを新たな第２秘密情報とすることを決定するものであり、
前記第２装置が有する前記一部の第２秘密情報は、前記決定に基づいて、前記新たな第２秘密情報により更新されたものであることを特徴とする請求項５記載の秘密情報変更システム。

【請求項９】　前記第２装置は、前記複数個の第２秘密情報の内、一部の第２秘密情報を有するものであり、
前記管理装置は、前記複数の第１秘密情報の内、秘密性が保持されなくなったものを除外した残りの第１秘密情報の中から、どれかを採用して、それらを新たな第２秘密情報とすることを決定し、その決定された新たな第２秘密情報を前記第２装置に送信するものであり、
前記第２装置は、前記送信されてきた新たな第２秘密情報により既に有していた前記第２秘密情報を更新することを特徴とする請求項５記載の秘密情報変更システム。

【請求項１０】　前記第２装置は、前記複数個の第２秘密情報の内、一部の第２秘密情報を有するものであり、
前記複数の第１秘密情報の内、秘密性が保持されなくなったものを除外した残りの第１秘密情報の中から、どれかを採用して、それらを新たな第２秘密情報とすることを決定する管理装置を備え、
前記第２装置が有する前記一部の第２秘密情報は、前記決定に基づいて、前記新たな第２秘密情報により更新されたものであることを特徴とする請求項６記載の秘密情報変更システム。

【請求項１１】　前記第２装置は、前記複数個の第２秘密情報の内、一部の第２秘密情報を有するものであり、
前記複数の第１秘密情報の内、秘密性が保持されなくな

ったものを除外した残りの第１秘密情報の中から、どれかを採用して、それらを新たな第２秘密情報とすることを決定し、その決定された新たな第２秘密情報を前記第２装置に送信する管理装置を備え、
前記第２装置は、前記送信されてきた新たな第２秘密情報により既に有していた前記第２秘密情報を更新することを特徴とする請求項６記載の秘密情報変更システム。
【請求項１２】　前記再生手段により再生される記録媒体に、前記指示と矛盾する指示が記録されていた場合、その指示は無視されることを特徴とする請求項６記載の秘密情報変更システム。
【請求項１３】　前記秘密情報は、前記データ送信装置と前記データ受信装置の間で、前記データの送信の前に行われる認証動作に利用する秘密関数、秘密鍵、又は公開鍵であることを特徴とする請求項１又は２記載の秘密情報変更システム。
【請求項１４】　認証又は所定の処理に利用する第１秘密情報を、予め複数個有する秘密情報変更第１装置であって、
前記複数個の第１秘密情報に対応する複数個の第２秘密情報の内、全部又は一部の第２秘密情報を有し、その第２秘密情報を利用して、前記第１装置との間で前記認証を、又は前記所定の処理に対応する処理を行う第２装置又は、前記第１装置が利用していた前記第２又は第１秘密情報をどれに変更すべきであるかを伝える外部からの指示に基づいて、前記第２又は第１秘密情報が変更されるものであり、
前記外部からの前記指示を受けた一方の前記装置が、他方の前記装置に対して、前記指示に基づく前記秘密情報の変更を指示するものであることを特徴とする秘密情報変更第１装置。
【請求項１５】　認証又は所定の処理に利用するために第１装置が予め複数個有する第１秘密情報に対応する複数個の第２秘密情報の内、全部又は一部の第２秘密情報を有し、その第２秘密情報を利用して、前記第１装置との間で前記認証を、又は前記所定の処理に対応する処理を行う秘密情報変更第２装置であって、
前記第１装置又は前記第２装置が利用していた前記第１又は第２秘密情報をどれに変更すべきであるかを伝える外部からの指示に基づいて、前記第１又は第２秘密情報が変更されるものであり、
前記外部からの前記指示を受けた一方の前記装置が、他方の前記装置に対して、前記指示に基づく前記秘密情報の変更を指示するものであることを特徴とする秘密情報変更第２装置。
【請求項１６】　認証又は所定の処理に利用する第１秘密情報を、予め複数個有する秘密情報変更第１装置であって、
前記複数個の第１秘密情報に対応する複数個の第２秘密情報の内、全部又は一部の第２秘密情報を有し、その第２秘密情報を利用して、前記第１装置との間で前記認証を、又は前記所定の処理に対応する処理を行う第２装置の前記第２秘密情報又は、前記第１秘密情報を変更すべき旨を伝える外部からの指示があった場合、前記第２装置又は前記第１装置が、前記秘密情報をどれに変更するかを選定するものであり、
前記外部からの前記指示を受けた一方の前記装置が、他方の前記装置に対して、前記指示に基づく前記秘密情報の変更を指示するものであることを特徴とする秘密情報変更第１装置。
【請求項１７】　認証又は所定の処理に利用するために第１装置が予め複数個有する第１秘密情報に対応する複数個の第２秘密情報の内、全部又は一部の第２秘密情報を有し、その第２秘密情報を利用して、前記第１装置との間で前記認証を、又は前記所定の処理に対応する処理を行う秘密情報変更第２装置であって、
前記第１秘密情報、又は前記第２秘密情報を変更すべき旨を伝える外部からの指示があった場合、前記第１装置又は前記第２装置が、前記秘密情報をどれに変更するかを選定するものであり、
前記外部からの前記指示を受けた一方の前記装置が、他方の前記装置に対して、前記指示に基づく前記秘密情報の変更を指示するものであることを特徴とする秘密情報変更第２装置。
【請求項１８】　請求項１～１７の何れか一つに記載の各手段の全部又は一部の手段をコンピュータに実行させるためのプログラムを記録したことを特徴とする媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、秘密情報変更システム、秘密情報変更第１装置、秘密情報変更第２装置、及び媒体に関する。
【０００２】
【従来の技術】従来より、衛星放送で送られてくるテレビ番組等を、専用の受信機（以下、これを単に、ＳＴＢと呼ぶ）により受信して、そのＳＴＢに接続されたＶＴＲ装置で録画したり、テレビで視聴したりすることが行われている。
【０００３】この場合、放送されてくる映像・音声データの中には、例えば、記録が禁止されているものや、１回だけ記録可能とされている条件付きデータがある。従って、これらの条件が守られる為には、この条件を正しく認識して、正規に動作する装置をユーザ側が使用することが前提となる。
【０００４】そこで、ＳＴＢから、例えばＶＴＲ装置に対して、１回のみ記録可能なＡＶデータを送信する場合、先ず、そのＶＴＲ装置が、上記の様な正規な装置であるかどうかを確認するための認証動作が行われることになると考えられる。
【０００５】以下に、従来のＳＴＢ及びＶＴＲ装置の構

成とその認証動作を簡単に述べる。

【０００６】一般に、このようなＳＴＢとＶＴＲ装置には、上記認証動作を行う為に用いる共通の秘密関数Ｓが、予め格納されている。

【０００７】ＶＴＲ装置からＳＴＢに対して、ＡＶデータの送信要求があると、上述したように、先ず、ＳＴＢとＶＴＲ装置の間で、互いに上記秘密関数Ｓを用いて、次の様な、チャレンジ・レスポンス型認証と呼ばれる作業が行われる。

【０００８】即ち、先ず、ＶＴＲ装置からＳＴＢに対して、リクエスト（認証要求）が出される。これを受けたＳＴＢは、ＶＴＲ装置に対して、チャレンジｘ（応答要求）を出し、ＶＴＲ装置からの応答を待つ。又、ＳＴＢは、自己の秘密関数Ｓを用いて、上記ｘからＳ（ｘ）を生成する。尚、Ｓ（ｘ）との記載は、ｘを秘密関数Ｓにより暗号化したものを表すものとする。

【０００９】一方、ＶＴＲ装置は、自己の秘密関数Ｓを用いて、受信したチャレンジｘから独自にＳ（ｘ）を生成し、そのＳ（ｘ）をＳＴＢへ送る。

【００１０】ＳＴＢは、自ら生成したＳ（ｘ）と、ＶＴＲ装置から送られてきたＳ（ｘ）と比較して、一致すれば、ＶＴＲ装置が正規な装置であると判定し、ＡＶデータの送信を開始する。又、不一致であれば、ＶＴＲ装置が不正な装置であると判定し、ＡＶデータの送信は行わない。

【００１１】尚、ＳＴＢに複数の装置が接続されている場合、それら複数の装置が有する秘密関数は、全て同じである場合と、それぞれに固有のものである場合がある。後者の場合、ＳＴＢは、それら装置に固有の全ての秘密関数を備えており、認証に際し、認証の相手装置に対応する秘密関数を使用するものである。

【００１２】

【発明が解決しようとする課題】しかしながら、上記の様な認証方法では、不正者が、正規な装置の秘密関数Ｓをそっくりそのまま模倣して、上記と同じ認証方法を行える不正な装置を製造・販売し、その不正装置が使用された場合、上記認証方法では、その装置が不正な装置であることを見破ることが出来ない。そこで、仮に、秘密関数Ｓが不正者により悪用されていることが分かった場合、その不正装置の使用を阻止する対策としては、悪用されたその秘密関数Ｓを使用しないようにするしかない。そのため、使用が禁止された秘密関数Ｓを予め有している正規の装置までも使用出来なくなるという弊害が出るという課題が有った。

【００１３】本発明は、この様な従来の課題を考慮し、不正な装置の排除に伴う弊害を従来に比べてより少なく出来る秘密情報変更システム、秘密情報変更第１装置、秘密情報変更第２装置、及び媒体を提供することを目的とする。

【００１４】

【課題を解決するための手段】請求項１記載の本発明は、認証又は所定の処理に利用する第１秘密情報を、予め複数個有する第１装置と、前記複数個の第１秘密情報に対応する複数個の第２秘密情報の内、全部又は一部の第２秘密情報を有し、その第２秘密情報を利用して、前記第１装置との間で前記認証を、又は前記所定の処理に対応する処理を行う第２装置とを備え、前記第１又は第２装置が利用していた前記第１又は第２秘密情報をどれに変更すべきであるかを伝える外部からの指示に基づいて、前記第１又は第２秘密情報が変更されるものであり、前記外部からの前記指示を受けた一方の前記装置が、他方の前記装置に対して、前記指示に基づく前記秘密情報の変更を指示するものである秘密情報変更システムである。

【００１５】請求項２記載の本発明は、認証又は所定の処理に利用する第１秘密情報を、予め複数個有する第１装置と、前記複数個の第１秘密情報に対応する複数個の第２秘密情報の内、全部又は一部の第２秘密情報を有し、その第２秘密情報を利用して、前記第１装置との間で前記認証を、又は前記所定の処理に対応する処理を行う第２装置とを備え、前記第１又は第２秘密情報を変更すべき旨を伝える外部からの指示があった場合、前記第１又は第２装置が、前記秘密情報をどれに変更するかを選定するものであり、前記外部からの前記指示を受けた一方の前記装置が、他方の前記装置に対して、前記指示に基づく前記秘密情報の変更を指示するものである秘密情報変更システムである。

【００１６】請求項１４記載の本発明は、認証又は所定の処理に利用する第１秘密情報を、予め複数個有する秘密情報変更第１装置であって、前記複数個の第１秘密情報に対応する複数個の第２秘密情報の内、全部又は一部の第２秘密情報を有し、その第２秘密情報を利用して、前記第１装置との間で前記認証を、又は前記所定の処理に対応する処理を行う第２装置又は、前記第１装置が利用していた前記第２又は第１秘密情報をどれに変更すべきであるかを伝える外部からの指示に基づいて、前記第２又は第１秘密情報が変更されるものであり、前記外部からの前記指示を受けた一方の前記装置が、他方の前記装置に対して、前記指示に基づく前記秘密情報の変更を指示するものである秘密情報変更第１装置である。

【００１７】請求項１５記載の本発明は、認証又は所定の処理に利用するために第１装置が予め複数個有する第１秘密情報に対応する複数個の第２秘密情報の内、全部又は一部の第２秘密情報を有し、その第２秘密情報を利用して、前記第１装置との間で前記認証を、又は前記所定の処理に対応する処理を行う秘密情報変更第２装置であって、前記第１装置又は前記第２装置が利用していた前記第１又は第２秘密情報をどれに変更すべきであるかを伝える外部からの指示に基づいて、前記第１又は第２秘密情報が変更されるものであり、前記外部からの前記

指示を受けた一方の前記装置が、他方の前記装置に対して、前記指示に基づく前記秘密情報の変更を指示するものである秘密情報変更第２装置である。

【００１８】請求項１６記載の本発明は、認証又は所定の処理に利用する第１秘密情報を、予め複数個有する秘密情報変更第１装置であって、前記複数個の第１秘密情報に対応する複数個の第２秘密情報の内、全部又は一部の第２秘密情報を有し、その第２秘密情報を利用して、前記第１装置との間で前記認証を、又は前記所定の処理に対応する処理を行う第２装置の前記第２秘密情報又は、前記第１秘密情報を変更すべき旨を伝える外部からの指示があった場合、前記第２装置又は前記第１装置が、前記秘密情報をどれに変更するかを選定するものであり、前記外部からの前記指示を受けた一方の前記装置が、他方の前記装置に対して、前記指示に基づく前記秘密情報の変更を指示するものである秘密情報変更第１装置である。

【００１９】請求項１７記載の本発明は、認証又は所定の処理に利用するために第１装置が予め複数個有する第１秘密情報に対応する複数個の第２秘密情報の内、全部又は一部の第２秘密情報を有し、その第２秘密情報を利用して、前記第１装置との間で前記認証を、又は前記所定の処理に対応する処理を行う秘密情報変更第２装置であって、前記第１秘密情報、又は前記第２秘密情報を変更すべき旨を伝える外部からの指示があった場合、前記第１装置又は前記第２装置が、前記秘密情報をどれに変更するかを選定するものであり、前記外部からの前記指示を受けた一方の前記装置が、他方の前記装置に対して、前記指示に基づく前記秘密情報の変更を指示するものである秘密情報変更第２装置である。

【００２０】

【発明の実施の形態】以下に、本発明の実施の形態を図面を参照して説明する。

【００２１】（第１の実施の形態）図１は、本発明の一実施の形態における秘密情報変更システムの構成を示す構成図であり、以下に、同図を参照しながら、本実施の形態の秘密情報変更システム及び各装置の構成について述べる。

【００２２】同図に示す様に、アンテナ１１０は、放送通信用衛星からの放送電波を受信する手段であり、衛星放送受信機（以下、これを単に、ＳＴＢと呼ぶ）１２０は、受信した放送電波をＡＶデータ等に変換する手段である。この放送電波の中には、放送局（図示省略）が放送する通常のテレビ番組の他に、現在使用中の秘密関数を別の秘密関数に変更せよという内容の変更指示情報の放送も含まれている。この変更指示情報の放送は、秘密関数を管理している管理センター（図示省略）の指示の基に行われるものである。管理センターは、不正者によりある秘密関数が盗まれたという情報を得て、その秘密関数の秘密性が保持されなくなったと判断した場合に、この様な変更指示情報を放送するものである。又、この変更指示情報には、上記盗まれた秘密関数を使用中の装置の固有のＩＤ情報が付されている。尚、秘密関数は、各装置間の認証作業において使用されるものであり、これについては、更に後述する。

【００２３】伝送ライン１６０は、ＳＴＢ１２０とＶＴＲ装置１４０との間に設けられた伝送のためのバスラインである。

【００２４】次に、同図を参照しながら、ＳＴＢ１２０の内部構成について更に述べる。

【００２５】即ち、受信手段１２１は、アンテナ１１０と直結し、受信したデータの復調を行い、その受信データに施されている放送用スクランブルを解除し、更に、多重化されている受信データを分離する手段である。この受信データの中には、上述した変更指示情報が含まれている。尚、この変更指示情報の放送は、本実施の形態の様に他の番組放送の電波と多重化されていても良いが、単独で放送されてきても良い。

【００２６】変更指示情報検出手段１２５は、受信手段１２１から出力される信号の中から、自己の固有のＩＤ情報が付された変更指示情報のみを検出し、変更指示情報を検出した旨を秘密関数選定手段１２８に出力する手段である。秘密関数格納手段１２６は、８個の秘密関数Ｓ１～Ｓ８を予め格納している手段である。又、これら秘密関数Ｓ１～Ｓ８には、それぞれに対応する１～８の識別番号が与えられているものとする。秘密関数履歴情報格納手段１２７は、使用が禁止された秘密関数及び現在使用中の秘密関数の識別番号を格納する手段である。秘密関数選定手段１２８は、変更指示情報検出手段１２５からの指示を得て、秘密関数履歴情報格納手段１２７の内容を加味して、現在使用中の秘密関数を別の秘密関数に変更する手段である。即ち、秘密関数選定手段１２８は、秘密関数格納手段１２６から新たな秘密関数を一つ選定し、その秘密関数をその識別番号とともに読み出し、それらを秘密関数指定情報として認証手段１２３へ送る手段である。又、秘密関数選定手段１２８は、秘密関数履歴情報格納手段１２７の内容を更新する手段である。

【００２７】一方、暗号化手段１２２は、認証手段１２３からの指示に基づいて、予め備えた暗号化のためのワークキーＫｗにより、受信手段１２１から出力されてきたＡＶデータを圧縮状態のまま暗号化し、又、認証手段１２３により生成されたサブキーＫｓｕｂを用いて、ワークキーＫｗを暗号化する手段である。サブキーＫｓｕｂについては、後述する。尚、ここで、上記の様に暗号化されたワークキーＫｗをも端末装置へ送る必要があるのは、端末装置では、転送されてきたＡＶデータを復号化した上で、記録等することを前提としているからである。

【００２８】認証手段１２３は、ＡＶデータの転送要求

を行ったＶＴＲ装置との間で、ＶＴＲ装置が正規の装置であるかどうかを確かめる認証作業を、上記秘密関数指定情報に基づいて行う手段である。認証手段１２３は、上記認証を始める際に、上記秘密関数指定情報に含まれる識別番号の情報を、認証相手となるＶＴＲ装置１４０へ送る手段である。

【００２９】データ転送力手段１２４は、ディジタル・インタフェースとして知られているＩＥＥＥ１３９４である。データ転送手段１２４は、リアルタイム性の保証が必要となる映像や音声の様なデータの転送に適したアイソクロナス転送と、その必要のない認証用データやコマンド等の転送に適したアシンクロナス転送の２つの転送を行う手段である。

【００３０】次に、図１を参照しながら、ＶＴＲ装置１４０の内部構成について、更に述べる。

【００３１】同図に示すとおり、データ転送手段１４１は、データ転送手段１２４と同様のディジタル・インターフェースである。

【００３２】秘密関数格納手段１４５は、１６個の秘密関数Ｓ１～Ｓ１６を予め格納している手段である。又、これら秘密関数Ｓ１～Ｓ１６には、それぞれに対応する１～１６の識別番号が与えられているものとする。尚、これら秘密関数Ｓ１～Ｓ８は、上述した秘密関数格納手段１２６が有する秘密関数と、識別番号も含めて同じである。秘密関数指定情報抽出手段１４６は、伝送されてきた信号の中から識別番号情報を検出し、それを基に、秘密関数格納手段１４５から対応する秘密関数を抽出し、認証手段１４２へ出力する手段である。

【００３３】認証手段１４２は、秘密関数指定情報抽出手段１４６からの指示に基づいて、認証作業を行う手段である。又、認証手段１４２は、認証手段１２３が生成するものと同一のサブキーＫｓｕｂを生成し、復号化手段１４３へ出力する手段である。復号化手段１４３は、データ転送手段１４１から得た暗号化されたワークキーＫｗをサブキーＫｓｕｂにより復号化してワークキーＫｗを復元し、そのワークキーＫｗにより、暗号化されたＡＶデータを復号化する手段である。記録・再生手段１４４は、復号化されたＡＶデータを記録し、又、その記録データを再生する手段である。ここで、本発明の第１装置は、ＶＴＲ装置１４０に対応し、本発明の第２装置は、ＳＴＢ１２０に対応する。本発明の複数個の第１秘密情報は、秘密関数Ｓ１～Ｓ１６に対応する。又、本発明の複数個の第１秘密情報に対応する複数個の第２秘密情報は、本実施の形態では、上記複数個の第１秘密情報と同一のものである。又、本発明の複数個の第１秘密情報に対応する複数個の第２秘密情報の内、一部の第２秘密情報は、秘密関数Ｓ１～Ｓ８に対応する。

【００３４】以上の構成により、以下に、図１、図２（ａ），（ｂ）を参照しながら、本実施の形態の動作を述べる。

【００３５】本実施の形態では、既に使用が禁止された秘密関数が２つあるという前提で説明する。図２（ａ），（ｂ）は、秘密関数履歴情報格納手段の内容を示す模式図である。図２（ａ）では、既に使用が禁止された秘密関数Ｓ１，Ｓ２の識別番号が、１と２であること、そして、その禁止された時間的順番が、識別番号１，２の順番であることを示し、又、現在使用中の秘密関数Ｓ３の識別番号が３であることを示している。

【００３６】ステップ１０１：即ち、ＳＴＢ１２０とＶＴＲ装置１４０との間で、現在使用されている秘密関数Ｓ３が、不正者により盗まれたという情報を得た管理センターは、そのＳＴＢ１２０の固有のＩＤ情報を付した変更指示情報を放送するよう所定の放送局へ指示する。

【００３７】ステップ１０２：放送局が、上記変更指示情報を、現在放送中の通常の放送番組と多重化して放送し、その通常の放送番組の後、引き続き通常の放送番組Ａ，Ｂ，Ｃを多重化して放送する。

【００３８】ステップ１０３：ＳＴＢ１２０のアンテナ１１０で受信された放送データは、受信手段１２１により上記所定の処理が行われ多重化が分離されて暗号化手段１２２と変更指示情報検出手段１２５へ出力される。

【００３９】ステップ１０４：変更指示情報検出手段１２５は、受信手段１２１から出力されてくる信号の中に、自己の固有のＩＤ情報が付された変更指示情報があるかどうかをチェックする。ここでは、自己のＩＤ情報が付された変更指示情報の存在を検出するので、その旨を秘密関数選定手段１２８へ出力する。変更指示情報検出手段１２５より上記出力を得た秘密関数選定手段１２８は、先ず、秘密関数履歴情報格納手段１２７の内容（図２（ａ）参照）を読み出して、秘密性が確保できなくなった秘密関数の識別番号が１～３であることを把握する。次に、秘密関数格納手段１２６（図１参照）から、上記識別番号１～３の秘密関数を除く、残りの秘密関数の中から識別番号が４の秘密関数Ｓ４を選定し、それらを読み出して、秘密関数指定情報として認証手段１２３へ出力する。この秘密関数指定情報により、認証手段１２３では、内部メモリ１２３ａに保持されている秘密関数Ｓ３とその識別番号３が、秘密関数Ｓ４とその識別番号４により更新される。尚、本実施の形態では、新たな秘密関数の選定は、上述の通り、秘密関数格納手段１２６の識別番号の昇順に行われる。又、秘密関数選定手段１２８は、上記選定の結果により、図２（ｂ）に示す様に、秘密関数履歴情報格納手段１２７の内容を更新する。ここで、図２（ｂ）は、図２（ａ）と比較すると、識別番号３の秘密関数が使用禁止の関数として加わり、新たに使用する秘密関数の識別番号が４である状況を示した図である。

【００４０】ステップ１０５：一方、ＶＴＲ装置１４０では、放送番組Ａの録画を行うために、先ず、認証手段１４２が、データ転送手段１４１を介して、ＳＴＢ１２

０に対し、リクエストを行う。本実施の形態での認証は、認証に使用する秘密関数が外部からの指示に応じて変更される点を除いて、上述したものと同じチェレンジ・レスポンス型認証である。

【００４１】ステップ１０６：即ち、ＶＴＲ装置１４０からリクエストを受けたＳＴＢ１２０のデータ転送手段１２４は、その内容を認証手段１２３へ送る。認証手段１２３は、これに対して、チャレンジｘをＶＴＲ装置１４０へ送ると同時に、内部メモリ１２３ａに記録されている識別番号４番を読み出して、識別番号情報として送る。チャレンジｘは、乱数を発生させて生成される。

【００４２】ステップ１０７：ＶＴＲ装置１４０の秘密関数指定情報抽出手段１４６は、データ転送手段１４１に送信されてきた信号の中から、識別番号情報を検出し、その内容から識別番号として、４番という情報を読み取る。そして、その４番に対応する秘密関数Ｓ４を、秘密関数格納手段１４５から抽出し、認証手段１４２へ出力する。

【００４３】ステップ１０８：認証手段１４２は、この様にして送られてきた秘密関数Ｓ４を利用して、上記チャレンジｘからＳ４（ｘ）を生成して、それをレスポンスとしてＳＴＢ１２０へ送る。又、認証手段１４２は、チャレンジｘからサブキーＫｓｕｂ・ｘを生成し、復号化手段１４３に送る。

【００４４】ステップ１０９：ＳＴＢ１２０の認証手段１２３では、内部メモリ１２３ａに記憶された秘密関数Ｓ４を用いて独自に生成したＳ４（ｘ）と、ＶＴＲ装置１４０からのレスポンスのＳ４（ｘ）と比較する。比較の結果、この場合は、同一であると判断されて、認証が成立する。又、ＳＴＢ１２０の認証手段１２３は、この様に認証が成立した結果、チャレンジｘからサブキーＫｓｕｂ・ｘを生成する。このサブキーはステップ１０８で述べたものと同一である。

【００４５】以降、認証が成立した後の動作（ステップ１１０～１１１）は、本実施の形態の特徴的な動作ではないので、簡単に述べる。

【００４６】ステップ１１０：暗号化手段１２２は、認証成立の情報を認証手段１２３から得て、受信手段１２１から出力されてきた信号から放送番組Ａのみを対象にワークキーＫｗで暗号化する。又、暗号化手段１２２は、ワークキーＫｗを、サブキーＫｓｕｂ・ｘにより暗号化する。そして、これら暗号化されたＫｗ（放送番組ＡのＡＶデータ）と、Ｋｓｕｂ・ｘ（Ｋｗ）とをデータ転送手段１２４からＶＴＲ装置１４０へ送る。

【００４７】ステップ１１１：復号化手段１４３は、得られたサブキーＫｓｕｂ・ｘを用いて、上記送られてきたＫｓｕｂ・ｘ（Ｋｗ）を復号し、更に、復号されたＫｗを用いて、Ｋｗ（放送番組ＡのＡＶデータ）を復号する。復号化された放送番組ＡのＡＶデータは記録・再生手段１４４により記録される。

【００４８】ところで、秘密関数Ｓ３を盗んだ不正装置（図示省略）から、上記ステップ１０５で述べたものと同様のリクエストが有った場合について簡単に述べる。

【００４９】即ち、この場合、不正装置は、新たな秘密関数Ｓ４を知らないので、ＳＴＢ１２０からのチャレンジｘに対する、レスポンスは、Ｓ３（ｘ）しか生成できない。そのため、この様な装置からのレスポンスは、ＳＴＢ１２０が比較基準として用意している新たなＳ４（ｘ）と一致せず、認証が不成立となる。従って、この様な装置には、要求データの転送は行われず、以降の処理が打ち切られる。これにより、不正装置のみを完全に排除出来る。

【００５０】尚、管理センターからの変更指示が無い場合の、認証動作については、上記ステップ１０５～ステップ１１１と基本的に同じである。

【００５１】次に、上記秘密関数Ｓ４が、不正者により盗まれたという情報を管理センターが得た場合における、上記とは別の動作を述べる。

【００５２】管理センターは、秘密性が保持出来なくなり使用不可能となった秘密関数がある程度増えてくると、ＳＴＢ装置の製造メーカーに対して、次ロットのＳＴＢの生産時からは、秘密関数格納手段１２６の内容を更新するように指示する。この指示を受けて、製造メーカーでは、次ロットのＳＴＢを生産する場合、上記秘密関数Ｓ１～Ｓ１６の１６個の中から、既に使用不可能となった秘密関数Ｓ１～Ｓ４を除く、８個の秘密関数を新たに選定し、その識別番号と共に秘密関数格納手段１２６へ格納する（図３（ａ）参照）。図３（ａ）は、次ロットとして生産されるＳＴＢが内蔵する秘密関数格納手段の内容を示す模式図である。図３（ｂ）は、既に生産されたＳＴＢが内蔵している秘密関数格納手段の内容を示す模式図である。尚、この様に、ＳＴＢが内蔵する秘密関数格納手段の内容が更新されても、その更新が、あくまで、既に生産されたＶＴＲ装置に予め格納されている秘密関数の範囲内であるので、既存のＶＴＲ装置が使用できなくなるという問題は生じない。又、この様に、ＳＴＢが内蔵する秘密関数格納手段の内容を所定のタイミングで更新することにより、ＳＴＢをも、管理センターの管理下に置くことが出来得る。即ち、ここでは、ＳＴＢが不正装置である場合までは想定していないが、ＳＴＢをこの様に管理センターの管理下に置くことにより、例えば、管理センターからの変更指示に従わず、使用禁止の秘密関数を使用し続ける様な不正なＳＴＢが発生しにくい環境にすることが出来る。

【００５３】尚、上記実施の形態では、秘密関数格納手段１２６の内容の更新を、新たな装置の製造段階で行う場合について述べたが、これに限らず例えば、既存の装置に対して、新たな秘密関数を管理センターからの指示により放送局から放送波で送り、それを基に更新が行われる構成でも良い。この場合、図１における、受信手段

１２１及び変更指示情報検出手段１２５等が、上記機能に加えて、次の様な機能を有している必要がある。即ち、先ず、放送局から、秘密関数のデータを有する更新指示情報が放送されてくる。ここでは、更新指示情報の内容が、図３（ａ）に示すものと等価であり、秘密関数格納手段１２６の内容が図３（ｂ）と同じである場合を例として述べる。受信手段１２１は、この更新指示情報を受信し、他の放送データと分離して出力する。変更指示情報検出手段１２５は、受信手段１２１の出力から更新指示情報を検出し、その更新指示情報に含まれている秘密関数Ｓ５～Ｓ１２とその識別番号５～１２を抽出する。更に、その抽出した秘密関数とその識別番号により、秘密関数格納手段１２６の内容（図３（ｂ）参照）を更新する。その結果、秘密関数格納手段１２６の内容は、図３（ａ）に示した内容となる。その他の構成は、図１で述べたものと同様である。

【００５４】（第２の実施の形態）図４は、本発明の一実施の形態における秘密情報変更システムの構成を示す構成図であり、以下に、同図を参照しながら、本実施の形態の秘密情報変更システム及び各装置の構成について述べる。

【００５５】尚、本実施の形態では、ＳＴＢ４００とＤＶＤプレーヤー４２０とにより構成される秘密情報変更システムについて述べるが、図１で説明したものと同一のものには、同一の符号を付し、その詳細な説明を省略する。従って、ここでは、上記実施の形態との相違点を中心に述べる。本実施の形態における上記実施の形態との主な相違点は、次のような点である。

（１）変更指示情報が、ＤＶＤに記録されていること。

（２）その変更指示の内容が、使用すべき秘密関数の識別番号を指定するものであること。

（３）ＤＶＤプレーヤー４２０が、変更指示情報を検出し、秘密関数の選定を行うこと。

（４）そのため、ＤＶＤプレーヤー内の秘密関数格納手段４２４が有する秘密関数の数の方が、ＳＴＢ内の秘密関数格納手段４０４が有する秘密関数の数よりも少ないこと。

（５）ＤＶＤプレーヤー４２０によりＤＶＤからデータを読み出して、ＳＴＢ４００に接続されたモニター４１０で視聴する場合であって、不正なＳＴＢを排除することを想定していること。

【００５６】図４に示すように、ＳＴＢ４００とＤＶＤプレーヤー４２０は、データ転送手段４０５及び４２５により伝送ライン１６０を介して接続されている。データ転送手段４０５及び４２５は、上記実施の形態と同様、何れもＩＥＥＥ１３９４により構成されている。

【００５７】又、同図に示すように、ＤＶＤプレーヤー４２０の構成は、ドライブ４２１、データ解読手段４２２を新たに備えるなど下記の点を除いて、図１に示すＳＴＢ１２０と共通する。

【００５８】即ち、ドライブ４２１は、セットされたＤＶＤを回転駆動し、記録信号を読み出す手段である。又、データ解読手段４２２は、ドライブ４２１で読み出された信号からＡＶデータを解読する手段である。変更指示情報検出手段１２５は、ドライブ４２１より出力されてくる信号から変更指示情報を検出する手段である。又、秘密関数抽出手段４２４は、秘密関数選定手段１２８とは異なり、変更指示情報により指示された識別番号を基に、秘密関数格納手段４２３から秘密関数を抽出する手段である。従って、ここでは、図１で示した秘密関数履歴情報格納手段１２７は不要である。又、秘密関数格納手段４２３は、図１で述べた秘密関数と異なる秘密関数Ｓ１０１～Ｓ１０８及びその識別番号１０１～１０８を格納する手段である。又、認証手段１２３は、内部メモリ１２３ａに加えて、履歴メモリ１２３ｂを有している点は、図１と相違する。履歴メモリ１２３ｂは、使用が禁止された秘密関数の識別番号の履歴を記録する手段である。ここで、本発明の第１装置は、ＤＶＤプレーヤ４２０に対応し、本発明の第２装置は、ＳＴＢ４００に対応する。又、本発明の再生手段は、ドライブ４２１等を含む手段である。

【００５９】一方、同図に示すＳＴＢ４００の構成について述べる。

【００６０】即ち、秘密関数指定情報抽出手段４０６は、ＤＶＤプレーヤー４２０からの伝送信号の中から識別番号情報を検出し、それを基に、秘密関数格納手段４０４から対応する秘密関数を抽出し、認証手段４０１へ出力する手段である。又、復号化手段４０２は、認証手段４０１より送られてきたサブキーＫｓｕｂを利用して、暗号化されたワークキーＫｗを復号化し、更に、それを用いて暗号化されたＡＶデータを復号化し、デコーダ４０３へ送る手段である。ここで、識別番号情報は、第１の実施の形態で述べたものと基本的に同じである。尚、デコーダ４０３を除く、これら各手段は、図１で述べたＶＴＲ装置１４０における各手段の内の同一名称の各手段と基本的に同じものである。但し、秘密関数格納手段４０４が格納する秘密関数とその識別番号は、図１で述べた秘密関数と異なる秘密関数Ｓ１０１～Ｓ１１６及びその識別番号１０１～１１６を格納する手段である。

【００６１】又、デコーダ４０３は、復号化されたＡＶデータは、圧縮さたままであるので、これを伸張し、その伸張した信号をモニター４１０へ出力する手段である。尚、アンテナ１１０及び受信手段１２１は、図１で述べたものと同じであるが、受信手段１２１の出力は、デコーダ４０３へ送られる点が異なる。

【００６２】以上の構成において、次に、本実施の形態の動作を述べる。

【００６３】ここでは、現在使用されている秘密関数Ｓ１０１が不正者により盗まれたという情報を得た管理セ

ンターが、次に製造するＤＶＤ$_2$に対しては、通常のＡＶデータ以外に、識別番号１０２の秘密関数を使用せよという内容の変更指示情報を記録する様に、ＤＶＤの製造メーカーに指示し、それが製造された場面を考える。そして、その新たなＤＶＤ$_2$が視聴される場合について説明する。

【００６４】ステップ２０１：所望の映画を見るために、使用者がＤＶＤ$_2$をＤＶＤプレーヤ４２０にセットして、駆動スイッチ（図示省略）をＯＮする。これによりドライブ４２１が、ＤＶＤ$_2$を回転駆動させ、変更指示情報が記録されているかどうかを最初にチェックし、記録されていれば、それを検出し、秘密関数抽出手段４２４へ出力する。ステップ２０２：秘密関数抽出手段４２４は、変更指示情報の内容を調べる。ここでは、識別番号１０２の秘密関数を使用せよという内容であるので、秘密関数格納手段４２３の中から、その識別番号１０２に対応する秘密関数Ｓ１０２を抽出する。抽出した秘密関数Ｓ１０２とその識別番号１０２とを認証手段１２３へ送る。

【００６５】ステップ２０３：認証手段１２３が、この秘密関数抽出手段から送られてきた秘密関数Ｓ１０２とその識別番号１０２により、内部メモリ１２３ａに記録されている現在使用中の秘密関数Ｓ１０１とその識別番号１０１番を更新する。更に、履歴メモリ１２３ｂに、使用が禁止された秘密関数の識別番号として、１０１番を追加記録する。履歴メモリ１２３ｂの利用については、後述する。

【００６６】ステップ２０４：認証手段１２３が行う認証動作は、ＳＴＢ４００が正規な装置であるかどうかを認証するものである。又、認証手段１２３と認証手段４０１との間で行われる認証動作は、ステップ１０６～１０９で述べたチャレンジ・レスポンス型認証とほぼ同じである。

【００６７】但し、本実施の形態では、ＤＶＤプレーヤ４２０がＳＴＢ４００に対してチャレンジｘを送るものであり、第１の実施の形態の場合と、ＳＴＢとその接続装置との立場が逆転している。又、その際、内部メモリ１２３ａに記録されている識別番号１０２番を読み出して、識別番号情報としてチャレンジｘと共に送る。

【００６８】又、ＳＴＢ４００の秘密関数指定情報抽出手段４０６は、上記ステップ１０７における秘密関数指定情報抽出手段１４６と同様の動作を行うが、ここでは、識別番号情報の内容が、識別番号１０２番を示すものであるので、秘密関数格納手段４０４の中から、それに対応する秘密関数Ｓ１０２を抽出し、認証手段４０１へ出力する。

【００６９】又、認証手段４０１における、レスポンス及びサブキーＫｓｕｂ・ｘの生成は、上記ステップ１０８の内容と同じである。

【００７０】又、ＤＶＤプレーヤ４２０の認証手段１２３における認証の成否判定及びサブキーＫｓｕｂ・ｘの生成は、上記ステップ１０９の内容と同じである。

【００７１】ステップ２０５：認証が成立し、復号化手段４０２により復号化されたＡＶデータは、デコーダ４０３へ送られて、伸張処理されて、モニター４１０へ送られる。この様にして、使用者は、所望の映画を見ることが出来る。

【００７２】これにより、上記実施の形態の場合と同様、不正装置のみを排除出来る。

【００７３】次に、ＤＶＤ$_2$と比較すると旧タイプとなるＤＶＤ$_1$を視聴する場合について、簡単に述べる。

【００７４】このＤＶＤ$_1$には、識別番号１０１の秘密関数を使用せよという内容の変更指示情報が記録されているものとする。

【００７５】この場合、ステップ２０３の述べた内部メモリ１２３ａの更新の前に、次のような動作を行う。

【００７６】即ち、認証手段１２３は、上記更新の前に、履歴メモリ１２３ｂの内容と、更新内容を比較する。ここでは、既に、履歴メモリ１２３ｂには、識別番号１０１は、使用禁止として記録されている。従って、既に使用が禁止されているものを復活させることになると判断し、この場合には、上記更新は行わず、その様な変更指示情報は無視する。

【００７７】これにより、一旦、新タイプのＤＶＤを再生させた後は、旧タイプのＤＶＤを再生させる場合でも、秘密関数は、新しいものに維持できるので、不正装置の排除がより一層確実に行えるものである。

【００７８】尚、本実施の形態においても、ＤＶＤプレーヤ４２０が内蔵する秘密関数格納手段４２３の内容を、製造メーカーにおいて、所定のタイミングで更新することは、第１の実施の形態で述べた場合と同様に行える。

【００７９】（第３の実施の形態）図５は、本発明の一実施の形態における秘密情報変更システムの構成を示す構成図であり、以下に、同図を参照しながら、本実施の形態の秘密情報変更システム及び各装置の構成について述べる。

【００８０】本実施の形態では、ＳＴＢ５００に対して、上記実施の形態で述べたものと同様のＶＴＲ装置１４０及びＤＶＤプレーヤ４２０が、伝送ライン１６０を介して接続されている構成である。又、ＳＴＢ５００は、上記実施の形態で述べたＳＴＢ１２０とＳＴＢ４００の両方の機能を併せ持つ構成である。従って、上述したものと同じ構成のものには、同じ符号を付してその説明を省略する。

【００８１】ここでは、上記実施の形態との相違点を中心に述べる。本実施の形態における上記実施の形態との主な相違点は、次のような点である。

（１）ＳＴＢ５００が使用する秘密関数は、接続されている装置の種類によって異なるものであること。

（2）ＳＴＢ５００の認証手段５０１は、データ送受信の相手との関係により、使用する秘密関数を指示する立場と、逆に指示される立場の両方の立場を使い分ける様に構成されていること。即ち、ＳＴＢ５００からＶＴＲ装置１４０にＡＶデータを転送する場合の認証手段５０１は、その認証動作において、使用すべき秘密関数をＶＴＲ装置１４０に対し指示する立場となる。これに対して、ＤＶＤプレーヤ４２０から転送されてくる再生信号をモニター４１０に表示する場合の認証手段５０１は、その認証動作において、使用すべき秘密関数をＤＶＤプレーヤ４２０から指示される立場となる。これらそれぞれの動作は、上記実施の形態で別々に述べたものと同様であり、ここでは省略する。

【００８２】次に、管理センターの指示に基づき、放送局から、ＤＶＤプレーヤ４２０が使用する秘密関数の変更指示情報が有った場合について簡単に述べる。尚、この変更指示の内容は、使用すべき秘密関数の識別番号を指定する内容であるとする。

【００８３】この変更情報は、ＳＴＢ５００のアンテナ１１０を通り、受信手段１２１を経て、変更指示情報検出手段１２５に入ることは上述したものと同じである。変更指示検出手段１２５は、この変更指示の対象となる秘密関数が、ＳＴＢ５００自身が主体的に変更出来る立場にあるものに該当するかどうかを予め定められた基準から判断する。そして、この秘密関数は、ＳＴＢ５００自身が主体的に変更する立場にないものと判断して、上記変更指示情報は、データ転送手段４０５へ送られて、ＤＶＤプレーヤ４２０へ転送される。

【００８４】本実施の形態のＤＶＤプレーヤ４２０では、図４で示したデータ転送４２５と変更情報検出手段１２５の間に、図４では示していない信号の伝達ラインを新たに設けておくことにより、上記変更指示情報が変更指示情報検出手段１２５へ送られる。以降の動作は、ドライブ４２１から変更指示情報が出力されてきた場合と同様である。

【００８５】このように、本実施の形態においても、上記の場合と同様の効果が発揮される。

【００８６】ところで、上述した各実施の形態の何れか一つの実施の形態に記載の各手段の全部又は一部の手段の機能をコンピュータに実行させるためのプログラムを磁気記録媒体や光記録媒体などの媒体に記録したものを作成し、それを用いて、上記と同様の動作を行わせても良い。

【００８７】尚、上記上記実施の形態では、外部からの変更指示情報は、現在使用中のものを変更せよという場合、使用すべきものを指示してくる場合について述べたが、これに限らず例えば、使用すべき識別番号をアップせよ、換言すれば、使用すべき識別番号のバッジョンナンバーをアップせよでもく、各装置内部はこれに対応する構成としても良い。但し、このような昇順タイプの構成の場合、不正な指示を排除するため、例えば、現在使用中の識別番号が１番の時に、識別番号をいきなり８番にせよとの変更指示情報が有っても、これを無視し、識別番号２への変更しかしない様にしてもよい。

【００８８】又、上記実施の形態では、ＳＴＢと各装置との間で、それぞれが有する秘密関数の個数が、異なっている場合について述べたが、これに限らず例えば、個数は、双方とも同一でも良い。

【００８９】又、本発明の第１又は第２秘密情報は、上記実施の形態では、認証に利用する秘密関数であったが、これに限らず例えば、認証に利用する秘密鍵又は公開鍵、その他、鍵の生成の元になる鍵の種的なものでもかまわない。

【００９０】又、本発明の第１又は第２秘密情報は、上記実施の形態では、認証に利用する秘密関数であったが、これに限らず例えば、認証とは関係なく、転送すべきデータを暗号化するために使用するものであっても良い。この場合、認証手段は無くてもかまわない。

【００９１】又、上記実施の形態では、認証方法として、チャレンジ・レスポンス型の認証であり、使用すべき秘密関数の指示は、チャレンジと同時に行う場合について述べたが、これに限らず例えば、別のタイプの認証方法でもよく、又、認証方法の如何に関わらず、使用すべき秘密情報の指示を行うのは、秘密情報の変更に対して主導権を持っている装置である。

【００９２】又、上記実施の形態では、本発明の第１秘密情報と第２秘密情報が同じである場合について述べたがこれに限らず例えば、同一でなくても勿論良い。

【００９３】

【発明の効果】以上述べたところから明らかなように本発明は、不正な装置の排除に伴う弊害を従来に比べてより少なく出来るという長所を有する。

【図面の簡単な説明】

【図１】本発明の一実施の形態における秘密情報変更システムの構成を示す構成図

【図２】（ａ）、（ｂ）：同実施の形態における、秘密関数履歴情報格納手段の内容を示す模式図

【図３】（ａ）：本実施の形態における、次ロットとして生産されるＳＴＢが内蔵する秘密関数格納手段の内容を示す模式図

（ｂ）：本実施の形態における、既に生産されたＳＴＢが内蔵している秘密関数格納手段の内容を示す模式図

【図４】本発明の第２の実施の形態における秘密情報変更システムの構成を示す構成図

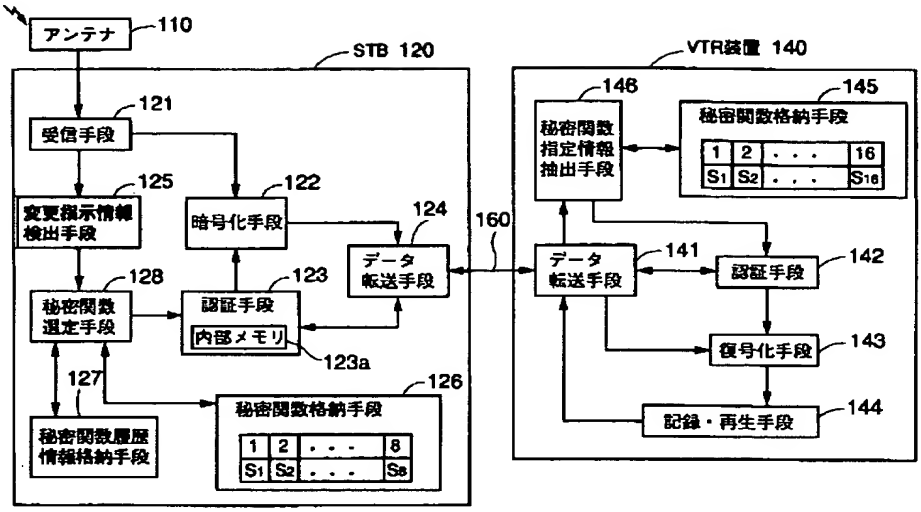
【図５】本発明の第３の実施の形態における秘密情報変更システムの構成を示す構成図

【符号の説明】

１１０　　アンテナ
１２０　　ＳＴＢ
１４０　　ＶＴＲ装置

１６０　伝送ライン
１２５　変更指示情報検出手段
１２１　受信手段
１２６　秘密関数格納手段
１２７　秘密関数履歴情報格納手段
１２８　秘密関数選定手段
１２３　認証手段
１２２　暗号化手段

【図１】



【図２】

(a)

現在使用中の秘密関数の識別番号	使用が禁止された秘密関数の識別番号
3	1
	2

(b)

現在使用中の秘密関数の識別番号	使用が禁止された秘密関数の識別番号
4	1
	2
	3

【図３】

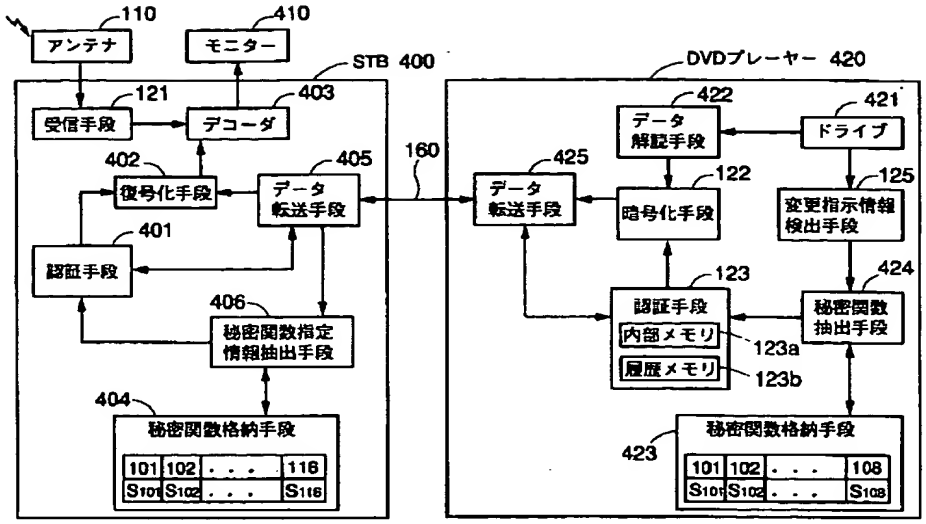
識別番号	5	6	7	8	9	10	11	12
秘密関数	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}

(a)

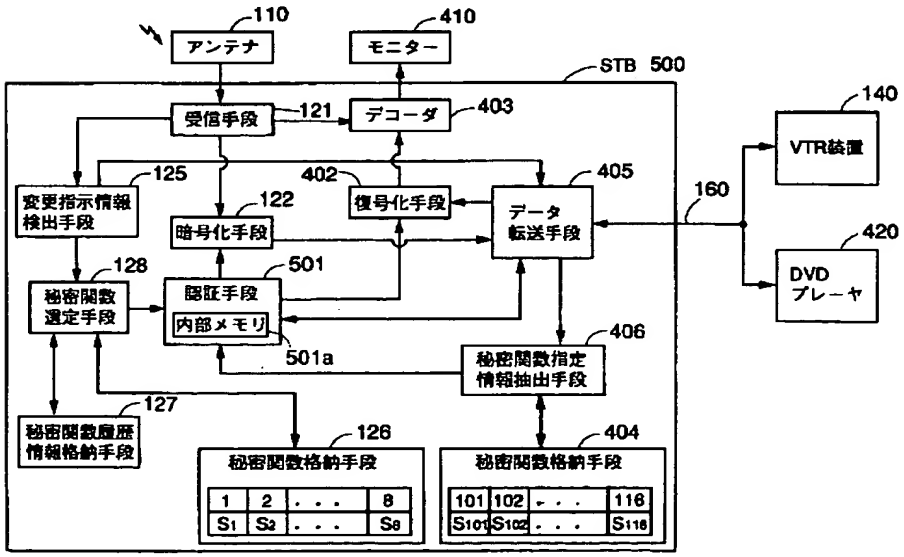
識別番号	1	2	3	4	5	6	7	8
秘密関数	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8

(b)

【図４】



【図５】



フロントページの続き

(72)発明者　後藤　昌一
大阪府門真市大字門真1006番地　松下電器
産業株式会社内